IN THE SPECIFICATION:

Please amend the specification as follows:

Please amend the paragraph beginning on Pg. 1, Line 28 as follows:

In IP-PBX, voice traffic is encapsulated inside IP packets and is carried between the IP phones using the LAN. For communications to phones in the public switched telephone network (PSTN), a gateway 130 is needed to convert the IP encapsulated voice traffic to the traditional time division multiplexed (TDM) format. The gateway 130 is also under control of the server 110 using H.248. The usual access protocol between the gateway 130 and the PSTN is ISDN PRI. Many traditional PBXs have been upgraded to have an IP interface to support IP phones. These PBXs are considered as IP-PBX in this convention.

Please amend the paragraph beginning on Pg. 2, Line 3 as follows:

As IP-PBXs are created, the need to connect all the PBXs within an enterprise together to form a corporate network exists (just as it did with respect to TDM based systems). An advantage in connecting two IP-based PBXs is that the voice traffic is already packetized. Direct packet-to-packet connectivity is desirable as there is no need to convert the voice packets to TDM and back to again. A packet to TDM gateway is not necessary for calls between the IP-PBXs. This results in cost reduction and improvement in the performance of the ~~system,~~ system, as this avoids costly packet to TDM conversion and vice versa.

Please amend the paragraph beginning on Pg. 2, Line 12 as follows:

In one of the approaches to interconnect IP-PBXs, the user subscribes to connection oriented packet services, such as frame relay and ATM permanent virtual circuit services, from a service provider (SP). The SP would only provide transport services for the ~~packer~~ packet and is not aware that the packets are voice packets. In an alternate approach in which the SP can provide added functionality, the SP would actively participate in the call signaling when a call is being in set up. In doing so, the SP can provide enhanced service at the request of the end-user on a call-by-call basis. As the

SP network is aware of when calls are set up and torn-down, the service can be charged based on call duration. This may result in lower cost to the end-user, another benefit. In the TDM environment, this alternative is similar to the "Software Defined Network" services from the SPs where TDM based PBXs are connected to the SP's networking using the Primary Rate Interface (PRI) from the ISDN. We will refer to this alternative as VoIP-VPN.

Please amend the paragraph beginning on Pg. 6, Line 22 as follows:

Fig. 2 depicts a portion of an exemplary communications system 200 in one embodiment of the subject invention. The system 200 comprises a Customer Premise 105 having a plurality of IP phones (101, 102, 103) and a server 110 connected to a VoIP-VPN SP at the SP's central office 205. Connection 145 is the connection between the ~~customer105 and CO 205, and~~ customer 105 and CO 205, and is made via one or more routers 140. In one embodiment of the invention, the subscriber (at the Customer Premise) uses their own IP address in assigning IP address to their devices. To increase reliability, dual access to the SP is possible (such as via a second connection 155 shown in broken line format).

Please amend the paragraph beginning on Pg. 7, Line 9 as follows:

Also located at the SP central office is a soft-switch 220. Server 110 at the Customer Premise 105 will communicate with the soft-switch 220 with an agreed upon signaling protocol. Examples of suitable protocols used are selected from the group consisting of H.248 and SIP. The soft-switch 220, based on requests from the server 110 or peer soft-switches (explained in greater detail below), sends the appropriate commands to packet switch 210 to set up the appropriate cross-connects. Such interaction between the soft-switch 220 and packet switch 210 is managed by a control interface (i.e., a vertical control interface) 215 (described in greater detail below). The soft-switch is the intelligence of the system. It contains all the information regarding the subscribers' VPNs. For example, it keeps track of the VPN that a ~~locations~~ location belongs to, the dial plans of the subscribers, the VPN identifier for an VPN (or a particular interface) and the like. The soft-switch can be implemented in a distributed manner in that its database

may be housed in a different physical unit than its processing logic modules or as a single unit. For simplicity, in the following descriptions, the soft-switch represents the entire system, containing all the necessary modules such as signaling, control logic, service logic, database and the like.

Please amend the paragraph beginning on Pg. 9, Line 31 as follows:

Note that the invention does not preclude direct logical connection between two "edge" packet switches 210. In fact, this is the case if the traffic volume between two packet switches warrants such a connection. More specifically, the invention supports both direct as well as consolidated (via core packet switches 402) connection. In addition, connectivity between the customer premise router 140 and the edge packet switch 210 as well as between packet switches do not ~~necessary based~~ necessarily need to be based on tunnel technologies. The invention also supports regular connectionless IP. However, in the latter case, quality of service may not be guaranteed.

Please amend the paragraph beginning on Pg. 10, Line 19 as follows:

The structure of the packet switch 210 is described herein for illustrative purposes only using the terminology of H.248. The logical structure of the packet switch 210 that manages voice traffic is depicted in Fig. 5. The packet switch 210 is provided with a plurality of layer-1 (physical) or layer-2 (logical link) connections 502, 504, 506. The peer of these connections can be routers 140 at customer premises 105, routers within the SF's IP network, and other packets switches (210 or 402). Each connection carries a number of voice calls. Each of the voice calls (denoted by arrows extending from the plurality of connections 502, 504 and 506 into the packet switch 210) passes through a VPN Processing Logic Module 510. The VPN Processing ~~Logic Module~~ Logic Module 510 decides how to establish the VPN based on the originating and destination addresses in the call signaling information (discussed in greater detail below). The maximum number of allowable calls for each connection depends on the amount of network resources allocated and the nature of the calls (coder, silence suppression, etc.). The soft-

switch 220 manages the number of active calls over a specific connection. Calls are identified as call terminations within packet switch 210.

Please amend the paragraph beginning on Pg. 12, Line 27 as follows:

The Call Terminations parameter identifies call termination and are identified as entities 512, 514, 516 and 518 in Fig. 5. The parameter has two sub-fields: IP address & UDP port number and VPN ID and other identifiers. With regard to IP address & UDP port number, in standard based VoIP implementation, voice traffic is encapsulated within IP/UDP/RTP packets. The packets are identified by their destination IP address, origination IP address, destination UDP port number, and origination UDP port number. With regard to VPN ID and other identifiers, in VoIP VPN, the subscriber can use their own IP addressing scheme. Therefore, an additional identifier is needed to indicate the VoIP VPN to distinguish the different IP address spaces. One embodiment of this identifier is to use the label of MPLS. The most interior MPLS label of a packet can be used to distinguish the VoIP VPN or even the egress interface (explained in greater detail below) at a packet switch 210, at the discretion of the SP. An alternate embodiment is to use the VPN ID as specified in RFC 2685 from the IETF. Just as the "layer-2 identifier" field in the "Connection End-Point" parameter described before, ~~addition identifier~~ additional identifiers may also be attached to support other enhanced features, (e.g. diverse routing). Therefore, this field is a sequence of identifiers in the form of (type, ID). The order of the sequence is significant, as this determines the meaning of the entry.

Please amend the paragraph beginning on Pg. 14, Line 3 as follows:

The sequence starts at step 602 when the user picks up the handset at phone 101. The phone will send an H.248 event to server 110 indicating that the phone is off-hook. At step 604, server 110 sends a H.248 "signal" command to IP phone 101 instructing the phone 101 to generate a dial tone to the user. At the same time, the server 110 also sends another message to instruct the IP phone 101 to begin to collect dialed digits from the user. At step 606, IP phone 101 collects dialed digits from the user and sends them to server 110 through H.248 "event" messages. The digits can be sent one at a time or "en block".

Please amend the paragraph beginning on Pg. 14, Line 12 as follows:

At step 608, after receiving all the dialed digits from the phone 101, server 110 consults its dial plan to determine whether the call is local, to another on-net phone, or to a phone that is on the PSTN. In this example, the call is to another on-net phone in another location. The server 110 then sends an SIP "invite" message to soft-switch 220 at the central office 205. There are many ways to encode the SIP message. In one embodiment, the server encapsulates the ISDN PRI "Set-up" message as a MIME (Multi-purpose Internet Mail Extension) object in the SIP message. PRI is the standard protocol between a PBX and a class-5 switch in the TDM environment; therefore, its encoding is well known. This method has the benefit that it preserves all existing features. Another embodiment is to encapsulate QSIG messages instead of PRI messages. QSIG is an enhanced version of PRI used between TDM based PBXs. The out-going call request message from server 110 to soft-switch 220 includes the following information, whether the protocol is SIP based or not: (1) the called number; (2) whether the number plan is the private numbering plan or the public E.164 number plan; (3) the ID of the connection to used (In this example, there is a single connection 145 between the customer premise 105 and the SP 205. In some instances, there could be multiple connections between the two and the server 110 can specify the one to be used. The server 110 can also have the option to allow the soft-switch 220 to select the connection to use.); (4) the IP address of IP phone 101 and UDP port number for the backward and forward channels; and (5) other parameters required for enhanced services and features. The server 110 also at the same time sends a H.248 command to the IP phone 101 to create a H.248 context for this call. The analog input and output from the hand-set is added to this context.

Please amend the paragraph beginning on Pg. 15, Line 5 as follows:

At step 610, upon receipt of the SIP "invite" message from the server 110, the soft-switch 220 consults the dial plan for this subscriber. The dial plan to use can be determined from the ID of the server 110. In this example, the call is to another on-net phone in another location. From the database associated with the dial plan, soft-switch 220 determines the following: (1) the IP address of the egress packet switch; (2) the

connection to use as the next hop for the bearer traffic; and (3) the IP address of the soft-switch of the next hop packet switch. Once the soft-switch 220 has determined this information, it sends H.248 commands to packet switch 210 instructing it to perform the following tasks: (1) create context 230 for this call; (2) add the call termination associated with call to the context just created (In this example, the call termination is identified by the following parameters: (1) connection end-point ID (the end-point ID associated with connection 145 at packet switch 210); (2) the IP address of the calling IP-phone (i.e., IP address A); and (3) UDP port address (as indicated in the SIP message, selected by the server 110 or the IP-phone 101, depending on implementation).

Please amend the paragraph beginning on Pg. 15, Line 30 as follows:

Fig. 7 depicts the sequence of signaling and control messages through the transit network 400. At this point, the soft switch 220 which manages the call from the originating server 110 is identified as an ingress soft switch, a soft switch 520 which manages the call to the terminating server 110 is identified as an egress soft switch and one or more intermediate soft switches 420 in the transit network 400 are identified as transit soft switches. Each soft switch 220, 420, 520 has a corresponding packet switch (i.e., ingress packet switch 210, transit packet switches 410 and egress packet switch ~~510.~~ 510). At step 616, upon the receipt of the SIP "invite" message from ingress soft-switch 220 from step ~~612, the~~ 612, the transit soft-switch 420 determines the following from the IP address of the egress packet switch 510: (1) the connection to use as the next hop for the bearer traffic; (2) the IP address of the soft-switch of the next hop packet switch. Once the transit soft-switch 420 has determined such information, it sends a H.248 command to transit packet-switch 410 instructing the packet switch to: (1) create context for this call; (2) add the call termination associated with call to the context just created (In this example, the call termination is identified by the following parameters: (1) connection end-point ID (the end-point ID associated with connection 240 at transit packet switch 410); (2) the IP address of the calling IP-phone; (3) VPN ID (i.e., 5); and (4) the UDP port address as indicated in the SIP message in step ~~612.~~ 612).

Please amend the paragraph beginning on Pg. 16, Line 18 as follows:

The processing of voice packets at a transit switch is simpler than that at the ingress or egress packet switch. As the ingress packet switch 210 has already inserted the identifier that identifies either the VPN or the egress interface. The only processing is for the soft-switch to determine the forwarding interface for the traffic of this call.

Please amend the paragraph beginning on Pg. 17, Line 3 as follows:

The forward signaling call flow continues at the egress soft-switch 520 as detailed in Figure 8. Specifically, at step 622, upon the receipt of the SIP message in step 618, soft-switch 520 recognizes that it is the egress soft-switch from the IP address of an egress packet. From the VPN ID field, it can determine the VPN that the call is for (i.e., VPN 5). It then consults the dialing plan for the VPN. From the called number, the soft switch 520 determines that the call is for a particular location (in this example, for a destination server 802 and over connection 540 at Destination Customer 806). It first sends H.248 commands to egress packet switch 510 to perform tasks as described in step 616. In addition, egress soft-switch 520 would instruct egress packet switch 510 to remove the VoIP-VPN identifier (or the egress interface ID) before forwarding the voice packets to a destination IP phone 601 over connection 540. Egress soft switch 520 and egress packet switch 510 form ~~and~~ an Egress SP Central Office 804.

Please amend the paragraph beginning on Pg. 17, Line 23 as follows:

At step 628, after the server 802 sends the command to called phone 601 to ring, it sends a SIP 100-response, "trying" to the egress switch 510 that the call has ~~reach~~ reached the end-terminal and the user has been alerted. This message will be propagated upstream to the ingress switch as Server 110 (shown as message 628a in Fig 8).

Please amend the paragraph beginning on Pg. 17, Line 32 as follows:

The sequence continues with the return signaling call flow at the egress soft-switch 520 as depicted in Fig. 9. Specifically, at step 632, when the called user picks up called (destination) phone 601, called phone 601 sends a H.248 "event" to server 802 indicating this action. At step 634, server 802 sends a SIP 200 response, "OK", to egress soft-switch 520 indicating that the user has picked up the phone. This message includes

the following information: (1) the IP address of the called IP-phone 601 and the UDP port number(s) for the backward and forward channels and (2) the connection used for the forward channel (the channel from the calling phone 101 to the called phone 601). In most cases, this would be the same channel as the one used for the back channel, especially [[IP]] if the channel is a bi-directional channel. In any case, the backward channel and the forward channel could be different and the invention allows this.

Please amend the paragraph beginning on Pg. 19, Line 14 as follows:

At the ingress and egress packet switch, an identifier specifying the VPN is inserted (or removed) between the RTP/IP/UDP packet and the lower layers. In the above example, MPLS label is used as the identifier. As presented earlier, other forms of identifiers such as VPN-ID can be used. This format will be used ~~with-in~~ within the SP's network. Figure 12 is an illustration of the encapsulation scheme for the channel at various points of the network. In one embodiment, packet switch 210 is connected to multiple VoIP-VPN locations belonging to different subscribers. For example, it can be connected to location 105 of subscriber A and location 106 of subscriber B (not shown). Subscriber A and B can each ~~uses~~ use their own addressing IP plan which may overlap. As such, ingress packet switch 210 needs to distinguish these packets. In the incoming side, the packet switch can identify the packets from the access connection (i.e. all packets from connection 145 belongs to subscriber A). As the packet switch would merge and forward packets from both subscribers on connection 240, towards the core network 310, a means to identify and separate these packets is necessary. In one embodiment of the invention, an identifier 1202 is inserted below an IP layer 1204 to identify the VoIP-VPN that the packets belong to. Specifically, an existing protocol stack 1210 of the voice packet changes from voice/RTP/UDP/IP/lower-layer to an improved protocol stack 1220 voice/RTP/UDP/IP/Identifier/lower-layers. An embodiment of this identifier is MPLS label. Another embodiment is the VPN-ID as specified in RFC 2685. Incoming packets from connection 240 would also contain this identifier. Base on the value of this identifier, packet switch 210, would identify the VoIP-VPN that the packet belongs to. It will remove the identifier 1202 and forward the packet to the appropriate location, consulting a VPN-specific forwarding table if necessary.

Please amend the paragraph beginning on Pg. 22, Line 18 as follows:

The configuration shown in Figure 14a is for calls between IP phones of different subscribers' networks (i.e. the first subscriber LAN 1304 and a second subscriber LAN ~~1404.~~ 1404). In such a scenario, both phones have a public E.164 number and an Inter-VPN gateway 1402 is used to interconnect the two phones 101 and 601. The inter-network operates like two PSTN gateway connected back-to-back, with all the TDM components removed. The major differences between an inter-network packet gateway ~~with~~ and a PSTN gateway are: (1) packets move in and out of the gateway with no TDM components or processing; (2) between the Inter-VPN packet gateway 1402 and IP phone 101, the packet gateway will use an IP address from the first subscriber's IP address space, and VPN identifier identifies subscriber 1 (or the egress interface to phone 101) and (3) there is a similar arrangement for IP phone 601 of subscriber 2. The inter-VPN will translate the IP address of phone 101 to another IP address from subscriber 2's IP address space, and the IP address of phone 601 to another IP address from subscriber 1's IP address space, when forwarding packets between the two phones. The translated IP addresses come from IP address polls allocated to the inter-VPN gateway, as described previously for the PSTN gateway.

Please amend the paragraph beginning on Pg. 24, Line 7 as follows:

Some ~~SP has~~ SPs have limited IP addresses. Therefore, in deploying VoIP services in ~~the~~ their access ~~network. This~~ network, this invention also applies in these situations. Basically, the access network is logically similar to a number ~~of IP-VPN~~ of IP-VPN locations, each with a server and using a private IP addressing plan.

Please amend the paragraph beginning on Pg. 24, Line 23 as follows:

There are many variations of implementation. One example is to assign a VPN-ID to each subscriber location. This results in all calls being inter-VPN calls. Then, splitting the inter-VPN gateway module 1402 to the ingress and egress packet switch. This results in double address translation for all calls (e.g., at the ingress as well as the egress switch). This implementation is more complex and uses more network resources. However, it

illustrates the flexibility and power of the invention. Fig. 15 is an illustration of this configuration and how address translation works.

Please amend the paragraph beginning on Pg. 24, Line 31 as follows:

Fig. 15 depicts a configuration for a call between two locations on the same ~~subsriber~~ subscriber where the above scheme is used to transfer traffic. In lieu of encapsulating the voice traffic using a VPN identifier, address translation by the split inter-VPN gateway at the ingress and egress packet switch is used. Referring to the figure, between IP phone A and the ingress packet switch 210, the IP address pair (destination and origination) would be A and B. Both addresses A and B are from the subscriber's IP address space. Similarly, the address pair between IP phone B and egress packet 510 is also A and B. The ingress soft-switch 220 knows of address B through the in-bound return signaling message (step 642), while the egress soft-switch 520 learns of the address B in the out-bound forward signaling message (step 622). Over the network, the address pair (A, B) will be converted to address pair (C. J). Both C and J are from the SP's own address space. The split gateway logical module in the packet switch would execute the conversion. Signaling messages would also be extended to carry addresses C and J. The above scheme also works even if the two phones are from different subscriber's network.